



# **Ruckus Wireless™ ZoneFlex™ 7025 Multimedia Wi-Fi Wall Switch**

## **User Guide**

For the following ZoneFlex 7025 Multimedia Wi-Fi Wall Switch models:

- 7025 Multimedia Wi-Fi Wall Switch (US)
- 7025 Multimedia Wi-Fi Wall Switch (EU)

Part Number 800-70273-001  
Published December 2010

[www.ruckuswireless.com](http://www.ruckuswireless.com)



# Contents

## About This Guide

Document Conventions .....	i
Related Documentation .....	ii
Documentation Feedback .....	ii

## 1 Introducing the 7025 Multimedia Wi-Fi Wall Switch

Overview of the 7025 Multimedia Wi-Fi Wall Switch .....	2
Unpacking the ZoneFlex 7025. ....	3
Package Contents .....	3
Getting to Know the ZoneFlex 7025 Features. ....	3
ZF7025-US Model .....	3
ZF7025-EU Model .....	6
LEDs .....	8
Reset Buttons .....	9

## 2 Installing the Multimedia Wi-Fi Wall Switch

Installing the ZF7025 .....	12
Step 1: Prepare the Administrative Computer .....	12
Step 2: Connect the Device to a Power Source and the Admin Computer ....	13
Step 3: Log In to the Device .....	14
Step 4: Configure the Wireless Settings .....	15
Step 5: Verify That the Wireless LAN is Operational .....	17
Physical Installation .....	18
Mount the ZoneFlex 7025 to the Outlet Box .....	18
Using the 110 Punch down Block .....	19

## 3 Navigating the Web Interface

Logging Into the Web Interface .....	22
Navigating the Web Interface. ....	23

## 4 Configuring the Multimedia Wi-Fi Wall Switch

Configuring Device Settings . . . . .	26
Configuring Internet Settings . . . . .	27
Default IP Addressing Behavior . . . . .	27
Obtaining and Assigning an IP Address . . . . .	27
Changing the Network Connection Type . . . . .	29
Renewing and Releasing DHCP . . . . .	29
Configuring Wireless Settings. . . . .	31
Configuring Common Wireless Settings . . . . .	31
Configuring Wireless # Settings . . . . .	36
Setting Threshold Options . . . . .	43
Rate Limiting. . . . .	45
Controlling Access to the Wireless Network . . . . .	46
Access Control Options . . . . .	46
Changing the Access Controls for a WLAN . . . . .	47
Removing a MAC Address . . . . .	48
Configuring LAN Ports. . . . .	48
Working with Port-Based VLANs . . . . .	50

## 5 Managing the Multimedia Wi-Fi Wall Switch

Viewing Current Wireless Settings . . . . .	52
Changing the Administrative Login Settings. . . . .	53
Configuring Management Access Options . . . . .	55
Enabling Logging and Sending Event Logs to a Syslog Server. . . . .	57
Sending a Copy of the Log File to Ruckus Wireless Support. . . . .	58
Saving a Copy of the Current Log to Your Computer . . . . .	58
Upgrading the Firmware . . . . .	59
Upgrading Manually via FTP or TFTP . . . . .	59
Upgrading Manually via the Web . . . . .	60
Upgrading Manually via Local File . . . . .	60
Scheduling Automatic Upgrades . . . . .	60
Rebooting the Multimedia Wi-Fi Wall Switch . . . . .	63
Resetting to Factory Defaults . . . . .	64
Running Diagnostics . . . . .	64
Where to Find More Information . . . . .	66

## Index



# About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless™ ZoneFlex™ 7025 Multimedia Wi-Fi Wall Switch. This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.



**NOTE:** If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at:

<http://support.ruckuswireless.com/>




## Document Conventions

[Table 1](#) and [Table 2](#) list the text and notice conventions that are used throughout this guide.

Table 1. *Text Conventions*

Convention	Description	Example
monospace	Represents information as it appears on screen	[Device name]>
<b>monospace bold</b>	Represents information that you enter	[Device name]> <b>set ipaddr 10.0.0.12</b>
<b>default font bold</b>	Keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Screen or page names	Click <b>Advanced Settings</b> . The <i>Advanced Settings</i> page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
	Information	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

## Related Documentation

In addition to this User Guide, each Ruckus Wireless 7025 Multimedia Wi-Fi Wall Switch documentation set includes the following:

- *Quick Setup Guide/Getting Started Guide*: Provides essential installation and configuration information to help you get the Multimedia Wi-Fi Wall Switch up and running within minutes.
- *Online Help*: Provides instructions for performing tasks using the Multimedia Wi-Fi Wall Switch's Web interface. The online help is accessible from the Web interface.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

Additionally, the ZoneDirector User Guide provides information on managing a ZoneFlex wireless network using a centralized Ruckus Wireless ZoneDirector WLAN controller. If you will be managing your ZoneFlex access points using ZoneDirector, refer to the ZoneDirector User Guide, available on the Ruckus Wireless website at <http://support.ruckuswireless.com/downloads>.

## Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

[docs@ruckuswireless.com](mailto:docs@ruckuswireless.com)

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:



- Ruckus Wireless ZoneFlex 7025 Multimedia Wi-Fi Wall Switch User Guide
- Part number: 800-70273-001
- Page 88



---

**NOTE:** Throughout this guide, the ZoneFlex 7025 Multimedia Wi-Fi Wall Switch may be referred to as "ZF7025," "Access Point," "AP" or simply, "device." All of these terms are synonymous for the purposes of this guide.

---



# Introducing the 7025 Multimedia Wi-Fi Wall Switch

## In This Chapter

<a href="#">Overview of the 7025 Multimedia Wi-Fi Wall Switch</a> .....	2
<a href="#">Unpacking the ZoneFlex 7025</a> .....	3
<a href="#">Getting to Know the ZoneFlex 7025 Features</a> .....	3

## Overview of the 7025 Multimedia Wi-Fi Wall Switch

Congratulations on your purchase of the Ruckus Wireless ZoneFlex 7025 Multimedia Wi-Fi Wall Switch!

The ZoneFlex 7025 Multimedia Wi-Fi Wall Switch is the industry's first wired and wireless wall switch that integrates high-speed 802.11n Wi-Fi into an ultra-sleek, low-profile design that can be quickly and discretely installed in a standard wall electrical outlet box.

The ZoneFlex 7025 delivers high performance 2.4GHz 802.11n wireless coverage and four wired Ethernet access connections that can be used to support a range of in-room IP device and user connectivity options. An additional passthrough port allows connectivity for digital phones that require native access to an in-house PBX system.

An IEEE 802.3af-compliant PoE port, up to 15.4 watts, powers devices such as IP telephones directly from the wall switch. The ZoneFlex 7025 requires only a single PoE cable drop, thereby reducing cabling, switch ports, and power sourcing equipment.

The ZoneFlex Multimedia Wi-Fi Wall Switch is completely inconspicuous, minimizing the protrusion off the wall to make in-room cabling and furniture arrangement simple. Flexible deployment options allow the ZoneFlex 7025 to be easily installed via two uplink Ethernet options: an RJ-45 Ethernet jack or a 110 punch down block connection. The ZoneFlex 7025 can be deployed as a standalone device or centrally managed by the Ruckus ZoneDirector or FlexMaster Wi-Fi system management platform.

Additionally, the ZoneFlex 7025 provides up to eight SSIDs per device, port-based VLANs, and Ruckus Wireless unique SmartCast™ traffic prioritization technology to ensure reliable performance for time-sensitive traffic such as video and VoIP.

Your ZoneFlex Access Point can be deployed in standalone mode or as part of the ZoneFlex Smart WLAN system, in which it can be managed by either FlexMaster or ZoneDirector WLAN controller.



---

**NOTE:** For more information on the ZoneFlex system (including FlexMaster and ZoneDirector), BeamFlex, and other Ruckus Wireless technologies, visit [www.ruckuswireless.com](http://www.ruckuswireless.com).

---

## Unpacking the ZoneFlex 7025

1. Open the ZoneFlex 7025 package, and then carefully remove the contents.
2. Return all packing materials to the shipping box, and put the box away in a dry location.
3. Verify that all items listed in [Package Contents](#) below are included in the package. Check each item for damage. If any item is damaged or missing, notify your authorized Ruckus Wireless sales representative.

### Package Contents

The contents of your ZoneFlex 7025 package includes the following:

- ZoneFlex 7025 unit
- Mounting bracket with two (2) mounting screws
- ZoneFlex 7025 Quick Start Guide
- Software License Agreement/Warranty Statement
- Regulatory flyer
- Registration card

## Getting to Know the ZoneFlex 7025 Features

This section identifies the physical features of each Multimedia Wi-Fi Wall Switch model that is discussed in this guide. Before you begin the installation process, Ruckus Wireless recommends that you become familiar with these features.

- [ZF7025-US Model](#)
- [ZF7025-EU Model](#)

### ZF7025-US Model

This section describes the physical features of the ZF7025-US model, which is designed to fit in a standard US-style wall electrical outlet box. The outlet box must conform to NEMA-WD6, with a minimum depth of 1.4 inches.

#### Front View Features

The front view of ZF7025-US, shown in [Figure 1](#), features a LAN port door which covers the four LAN ports, a pass through port and a DC in socket on the right side. Refer to [Table 3](#) for more information.

Figure 1. ZF7025-US front view

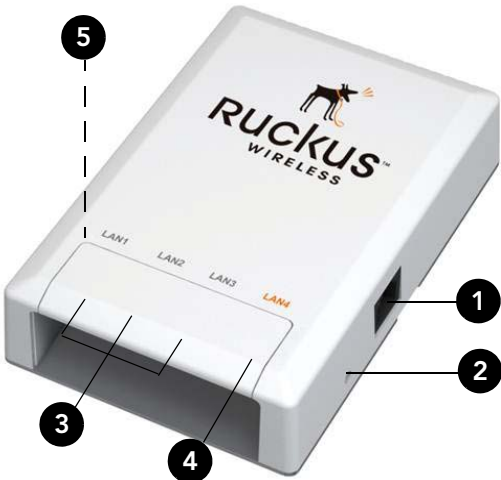


Table 3. ZF7025-US front view

Number	Name	Description
1	Pass Through port	Pass through port.
2	Power Input	Optional 48V DC power input.
3	LAN1-LAN3	Three 10/100 RJ-45 LAN ports.
4	LAN4	One 10/100 RJ-45 LAN port with PoE out. Supports 802.3af PSE Class 0/2 (depending on power input).
5	Reset Buttons (left side)	Refer to <a href="#">"Reset Buttons"</a> on <a href="#">page 9</a> for details.

### Rear Panel Features

[Figure 2](#) shows the rear panel of the ZF7025-US model. For a description of each rear panel element, refer to [Table 4](#).

Figure 2. ZF7025-US rear panel

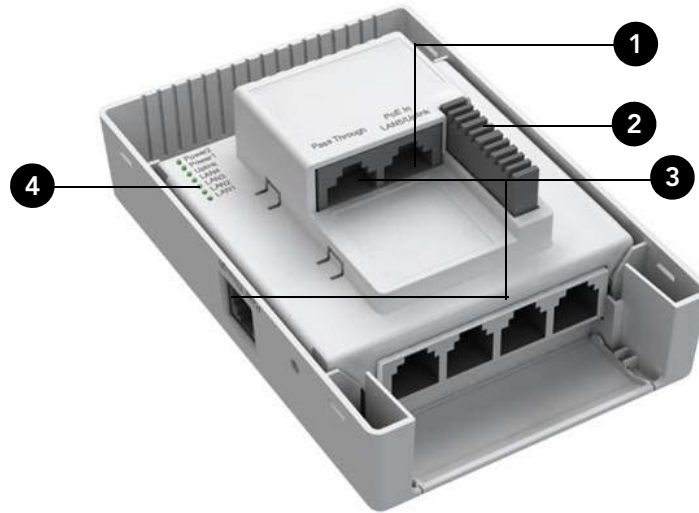


Table 4. ZF7025-US rear panel features

Number	Name	Description
1	PoE In LAN 5/Uplink	Uplink LAN port that supports 802.3af and 802.3at Power over Ethernet (PoE) input.
2	Punch down Block	110 punchdown block.
3	Pass Through Port	RJ-45 pass through port for the pass through connection.
4	LEDs	See <a href="#">Table 7</a> for LED descriptions and behaviors.

## ZF7025-EU Model

This section describes the physical features of the ZF7025-US model, which is designed to fit in a standard EU-style wall electrical outlet box. The outlet box must conform to BS 4662, with a minimum depth of 35mm.

### Front View Features

[Figure 3](#) shows the front view of the ZF7025-EU model. For a description of each front view element, refer to [Table 5](#).

Figure 3. ZF7025-EU front view

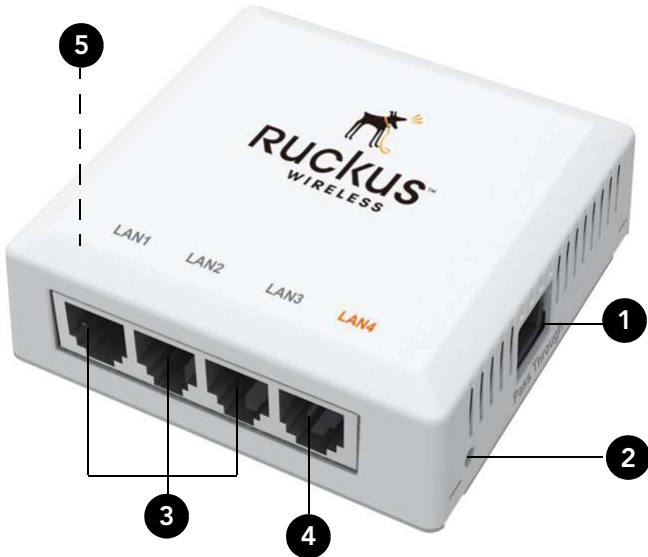


Table 5. ZF7025-EU front view

Number	Name	Description
1	Pass Through port	Pass through port.
2	Power Input	Optional 48V DC power input.
3	LAN1-LAN3	Three 10/100 RJ-45 LAN ports.
4	LAN4	One 10/100 RJ-45 LAN port with PoE out. Supports 802.3af PSE Class 0/2 (depending on power input).
5	Reset Buttons (left side)	Refer to <a href="#">"Reset Buttons"</a> on <a href="#">page 9</a> for details.



Rear View Features

[Figure 4](#) shows the rear panel of the ZF7025-EU model. For a description of each rear panel element, refer to [Table 7](#).

Figure 4. ZF7025-EU rear panel



Table 6. ZF7025-EU rear panel features

Number	Name	Description
1	PoE In LAN 5/Uplink	Uplink LAN port that supports 802.3af and 802.3at Power over Ethernet (PoE) input.
2	Punch down Block	110 punchdown block.
3	Pass Through Port	Uplink RJ-45 pass through port for the pass through connection.
4	LEDs	See <a href="#">Table 7</a> for LED descriptions and behaviors.

## LEDs

The LEDs for both the US and EU models are the same. Refer to [Table 7](#) for descriptions of LEDs and their behaviors. The LEDs are not visible once the AP is installed.

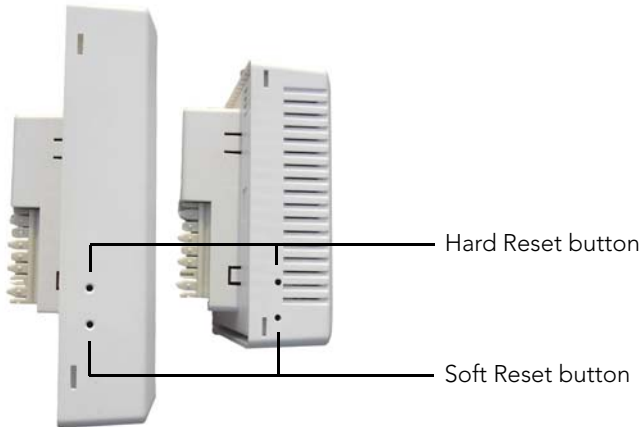
Table 7. ZF7025 LEDs

LED	Meaning
WLAN	Green: WLAN service is available. Off: No WLAN service available.
OPT	Not used in this model.
DIR	Green: AP is being managed by ZoneDirector. Off: AP is not being managed by ZoneDirector.
Power	Green: On Red: Bootup in process Off: Off
LAN5/Uplink	Green: Link up. Flashing green: Activity. Off: Link down.
LAN1 - LAN4	Green: Link up. Flashing green: Activity. Off: Link down.

## Reset Buttons

Two reset buttons on the left side of the AP are used to reboot or factory reset the AP.

*Figure 5. Reset buttons*



Press and release either of the reset buttons to reboot the AP. Press and hold the Hard Reset button for three seconds or more to reset the AP to factory defaults.

## Introducing the 7025 Multimedia Wi-Fi Wall Switch

Getting to Know the ZoneFlex 7025 Features

# Installing the Multimedia Wi-Fi Wall Switch

## In This Chapter

<a href="#">Installing the ZF7025</a> .....	12
<a href="#">Associate a Wireless Client with the Access Point</a> .....	18
<a href="#">Physical Installation</a> .....	18

## Installing the ZF7025

Before starting with the installation, make sure that you have the following items that are required for the installation ready:

- A computer with a Web browser
- Two CAT5 Ethernet cables
- An IEEE 802.3af/at-compliant PoE switch or PoE injector and power adapter

### Step 1: Prepare the Administrative Computer

The administrative computer is the computer that you will be using to access the device's Web interface.



**NOTE:** These procedures assume that the admin computer is running Windows XP or Windows 7 operating system. Procedures for other operating systems are similar.

1. Power on your computer.
2. Go to the network connection settings.
  - On Windows XP, click **Start > Settings > Control Panel > Network Connections**.
  - On Windows 7, click **Open Network and Sharing Center > Change Adapter Settings**
3. Double-click the icon for **Local Area Connection**.
4. In the Local Area Connection Properties window,
  - On Windows XP, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
  - On Windows 7, click **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
5. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.
6. Select **Use the following IP address**, and then configure the IP address settings with the values listed in [Table 8](#). For a sample configuration, refer to Figure 19.
7. Click **OK** to exit the Local Area Connection Properties window.

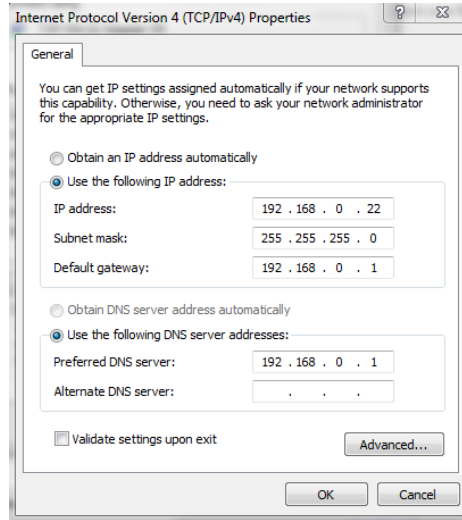
Table 8. Configure your computer's IP address

IP address	192 . 168 . 0 . 22 (or any address in the 192.168.0.xx range, with the exception of 192.168.0.1, which is the default IP address of the AP).
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 0 . 1
Preferred DNS server	192 . 168 . 0 . 1

You can leave the **Alternate DNS server** box blank.

8. Click **OK** to save your changes and close the TCP/IP Properties dialog box.
  9. Click **OK** again to close the Local Area Connection Properties dialog box.
- Windows saves the IP address settings that you have configured.

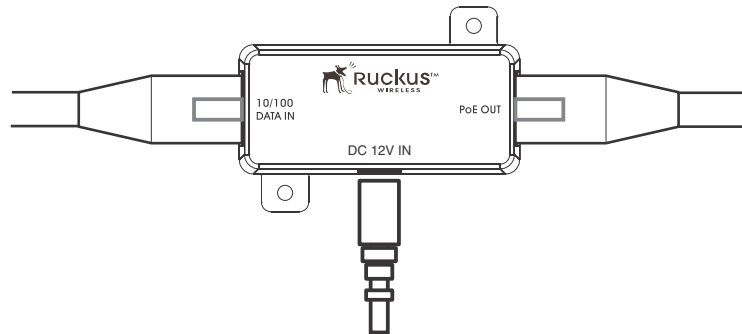
Figure 6. Sample configuration in the TCP/IP Properties dialog box



## Step 2: Connect the Device to a Power Source and the Admin Computer

1. Connect the AP to an 802.3af or 802.3at compliant PoE injector or PoE switch.
2. If using a PoE injector, see [Figure 7](#) for connections.

Figure 7. Connect the Ethernet cables and power adapter to the PoE injector



3. Take one of the CAT5 Ethernet cables. Connect one end of the Ethernet cable to the Ethernet port on your computer, and then connect the other end to the **10/100 DATA IN** port on the PoE injector.
4. Take the other Ethernet cable. Connect one end to the **PoE OUT** port on the PoE injector, and then connect the other end to the **PoE In LAN 5/Uplink** port on the rear of the device (see [Figure 8](#)).

Figure 8. Rear panel of ZF7025

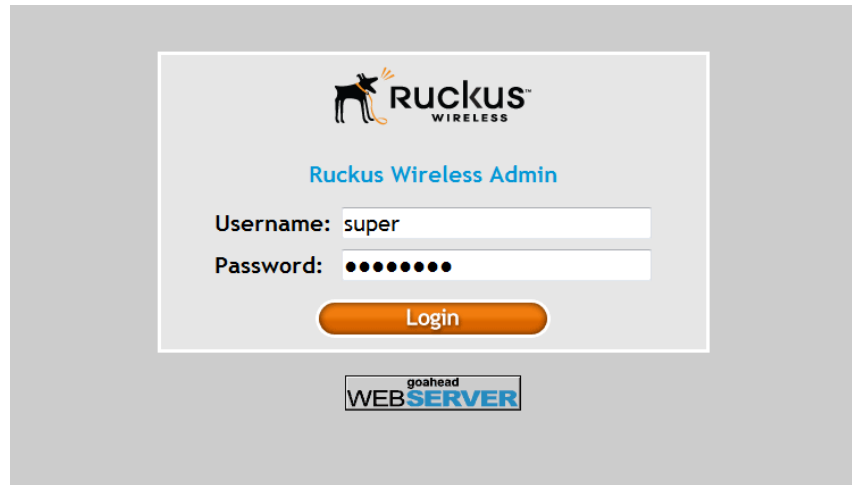


### Step 3: Log In to the Device

1. On your computer, open a Web browser window.
2. In the address or location bar, enter **192.168.0.1**.
3. When the login screen appears, type **super** as the user name and **sp-admin** as the password.



Figure 9. Web interface login page



4. Click the **Login** button. The *Status :: Device* page appears.
5. Continue to ["Step 4: Configure the Wireless Settings"](#).

## Step 4: Configure the Wireless Settings

To complete this step, you will need to configure the settings on the **Common** tab and at least one **Wireless #** tab. These are the essential wireless settings that will enable wireless devices on the network to associate with the Access Point.

For your reference, the default wireless settings on the Access Point are listed in [Table 9](#).

Table 9. Default Wireless Settings

Setting	Default Value
SSID (network name)	Wireless 1 to Wireless 8 (8 WLANs)
Encryption (security)	Disabled on all WLANs
Default management IP address	192.168.0.1

### Configure Common Wireless Settings

1. On the left menu of the Web interface, click **Configuration > Wireless**. The **Configuration :: Wireless :: Common** page appears.

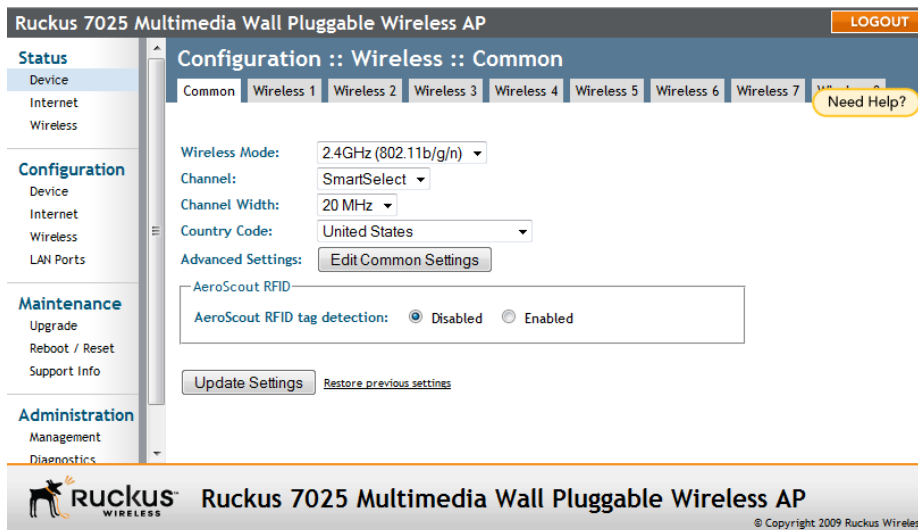
2. Verify that the common wireless settings are configured as listed in [Table 10](#).

Table 10. Common wireless configuration

Setting	Recommended Value
Wireless Mode	2.4GHz (802.11b/g/n) (not configurable).
Channel	SmartSelect
Channel Width	20MHz
Country Code	<ul style="list-style-type: none"> <li>• If you purchased the Access Point in the United States, this value is fixed to United States at the factory and is not user configurable.</li> <li>• If you purchased the Access Point outside the United States, verify that the value is set to your country or region. Selecting the correct country code ensures that the Access Point uses only the radio channels allowed in your country or region.</li> </ul>
AeroScout RFID tag Detection	Disabled

3. If you made any changes to the Common tab, click Update Settings.
4. Continue to [Configure Wireless # Settings](#) below.

Figure 10. The Configuration :: Wireless :: Common tab



### Configure Wireless # Settings

1. Click one of the **Wireless #** tabs.
2. In **Wireless Availability**, click **Enabled**.
3. In **Broadcast SSID**, click **Enabled**.
4. Clear the **SSID** box, and then type a unique and descriptive name that you want to call this wireless network.

For example, you can type `Ruckus Wireless AP`. This SSID is the name that will help users identify this wireless network in their wireless network connection application.



**NOTE:** You may also configure other wireless settings on this and other **Wireless #** tabs (in addition to the settings described above), although it is not necessary for completing the Access Point installation.

5. Click **Update Settings**.

You have completed configuring the basic wireless settings of the Access Point.

Figure 11. The Configuration :: Wireless :: Wireless 1 tab

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

Configuration :: Wireless :: Wireless 1

Wireless Network: Wireless 1

Wireless Availability? ☒ Enabled ☐ Disabled

Broadcast SSID? ☒ Enabled ☐ Disabled

SSID: Wireless1

Threshold Settings: Edit Settings

Rate Limiting: Edit Settings

Access Control: Edit Settings

VLAN: ☒ No VLAN ☐ VLAN ID

Encryption Method: Disabled

Update Settings Restore previous settings


Ruckus WIRELESS Ruckus 7025 Multimedia Wall Pluggable Wireless AP


© Copyright 2009 Ruckus Wireless

## Step 5: Verify That the Wireless LAN is Operational

After you have enabled a wireless LAN, you should be able to access the WLAN using a notebook computer through its wireless interface.

## Associate a Wireless Client with the Access Point

1. On the administrative computer, verify that the wireless interface is enabled. On Windows XP, click **All Programs > Connect To > Wireless Network Connection** to enable the wireless interface.
2. In the system tray, right-click the  (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
3. In the list of available wireless networks, click the network with the same SSID as you configured in ["Configure Wireless # Settings"](#) on [page 17](#). For example, if you set the SSID to Ruckus Wireless AP, click the wireless network named **Ruckus Wireless AP**.
4. Click **Connect**.

Your wireless client connects to the wireless network. After the wireless client connects to the wireless network successfully, the wireless client icon in the system tray changes to .

## Physical Installation



---

**CAUTION:** The AP and all interconnected equipment must be installed indoors within the same building, including the PoE powered network connection as described by Environment A of the 802.3af standard.

---



---

**CAUTION:** Ensure that you use a Cat5e or better Ethernet cable to supply PoE power and LAN connectivity running to the outlet box where the AP will be installed.

---

## Mount the ZoneFlex 7025 to the Outlet Box

1. Prepare the electrical outlet box.

The ZoneFlex 7025 requires a single-gang electrical outlet box mounted in a wall cavity. The US version requires a box conforming to NEMA-WD6, with a minimum depth of 1.4 inches. The EU version requires a box conforming to BS 4662, with a minimum depth of 35mm.

- Remove the outlet box cover from the outlet box.
- Run the required cables through the electrical outlet box allowing sufficient slack for the cables to reach the not yet installed ZoneFlex 7025.

2. Connect the cables

- Connect an Ethernet cable providing PoE power and network connectivity to the **PoE In LAN 5 / Uplink** port using either a standard RJ-45 connector or the 110 punch-down block. **Do not connect both.** (See ["Using the 110 Punch down Block"](#) on [page 19](#) for punch-down block wiring details).

- If required, connect the cable providing support for pass-through devices to the **Pass Through** port.
3. Mount the ZoneFlex 7025.
- Align the mounting bracket with the outlet box so that the two screw holes line up, and pull the Ethernet cable through the center of the mounting bracket.
  - Affix the mounting bracket to the outlet box using the two mounting screws provided.
  - Snap the AP onto the mounting bracket by hooking the two locking tabs on one side of the mounting bracket into the two cutouts in the plastic housing on one side of the AP, then push the other side of the AP in toward the wall until it snaps in place.

Figure 12. Hook the locking tabs into the housing cutouts



You have completed the physical installation.

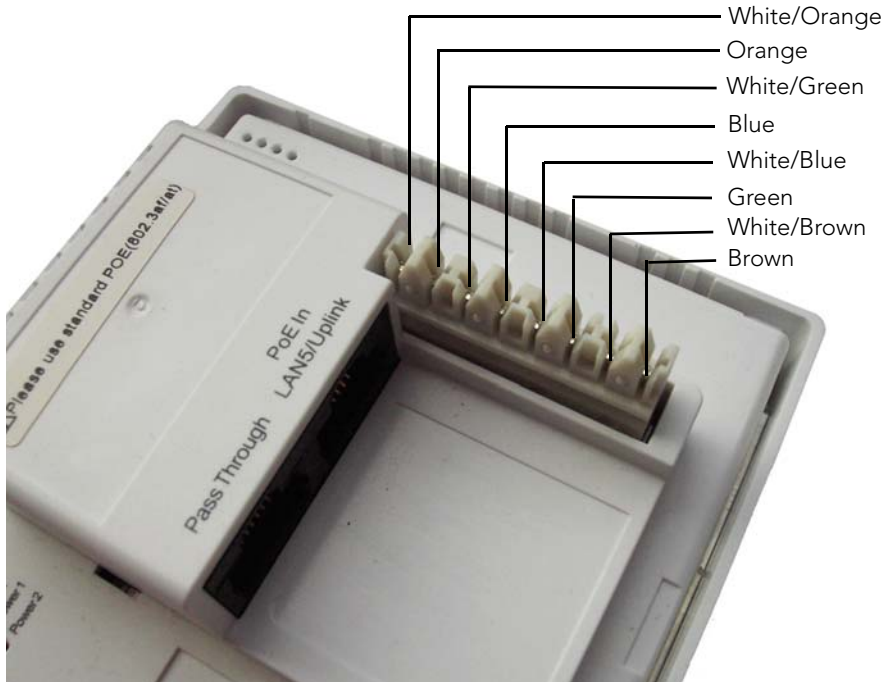
## Using the 110 Punch down Block



**CAUTION:** Do not connect both the Punch-down block and the Uplink port to a network. Only one connection can be used at a time.

If you prefer to use the 110 Punch-down block connector rather than the RJ-45 connector for power and network connectivity, refer to the following diagram for wiring details.

Figure 13. *Punch-down block wiring*



*Congratulations! Your wireless network is now active and ready for use.*

- If you want to become familiar with the Multimedia Wi-Fi Wall Switch Web interface, refer to [“Navigating the Web Interface”](#) on [page 21](#).
- If you want to perform additional configuration tasks (such as configuring the system and wireless settings and controlling access to the wireless network), refer to [“Configuring the Multimedia Wi-Fi Wall Switch”](#) on [page 25](#).
- If you want to perform management tasks (such as changing the administrative password, upgrading the firmware, or running diagnostics), refer to [“Managing the Multimedia Wi-Fi Wall Switch”](#) on [page 51](#).

# Navigating the Web Interface

**In This Chapter**

<a href="#">Logging Into the Web Interface</a> .....	22
<a href="#">Navigating the Web Interface</a> .....	23

## Logging Into the Web Interface

If you need to manage the device, you do it with the features of the Ruckus Wireless Web interface (which you already used to set up the device for use).



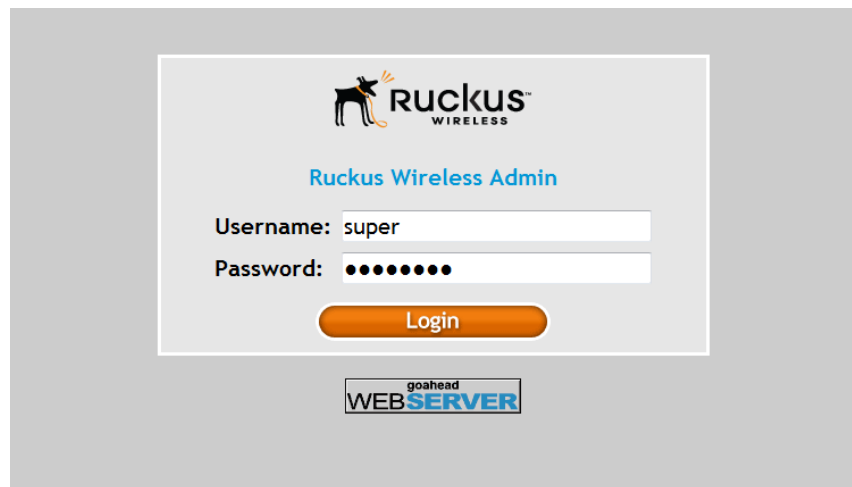
**NOTE:** The following procedure assumes that you know the IP address that the device is currently using, or you have some means of determining the dynamic IP address in use by the device. The computer that you will use to access the Web interface must be on the same subnet as the Ruckus Wireless device.

### To log into the Web interface

1. On your computer, open a Web browser window.
2. In the address or location bar, type the IP address of the device. Be sure to enter it in the format:  
`http://<ip_address>`
3. Press <Enter> to connect to the Web interface.
4. If a Windows security alert dialog box appears, click **OK/Yes** to proceed. The Ruckus Wireless Admin login page appears.
5. In **Username**, type `super`.
6. In **Password**, type `sp-admin`.
7. Click **Login**.

The Multimedia Wi-Fi Wall Switch Web interface appears.

Figure 14. Login page of the Web interface





## Navigating the Web Interface

You manage the Multimedia Wi-Fi Wall Switch through a Web browser-based interface that you can access from any computer that is on the same subnet as the Multimedia Wi-Fi Wall Switch. [Table 11](#) lists the Web interface features that are identified in [Figure 15](#).

Figure 15. Elements of the 7025 Multimedia Wi-Fi Wall Switch Web Interface

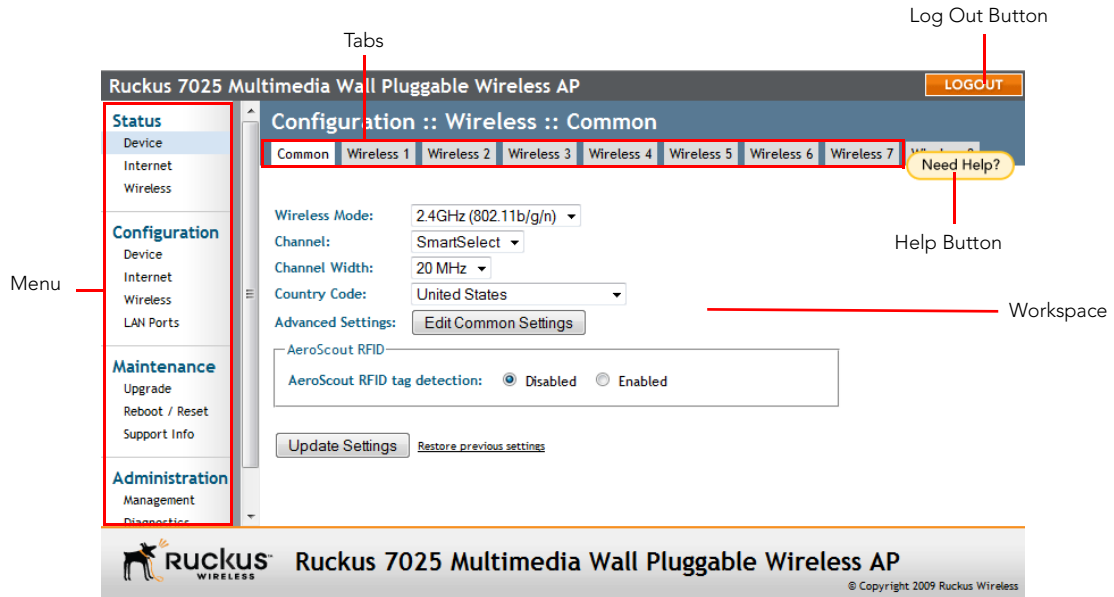


Table 11. 7025 Multimedia Wi-Fi Wall Switch Web interface elements

Element	Description
Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
Tabs	Contains additional options for the configuration page. For example, the <b>Configuration &gt; Wireless</b> page includes one tab for common wireless configuration and eight tabs for each of the available WLANs.
Workspace	This large area displays features, options and indicators relevant to the menu item that you clicked.

*Table 11. 7025 Multimedia Wi-Fi Wall Switch Web interface elements*

Element	Description
Logout Button	Click this button to log out of the Multimedia Wi-Fi Wall Switch.
Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.

# Configuring the Multimedia Wi-Fi Wall Switch

## In This Chapter

<a href="#">Configuring Device Settings</a> .....	26
<a href="#">Configuring Internet Settings</a> .....	27
<a href="#">Configuring Wireless Settings</a> .....	31
<a href="#">Controlling Access to the Wireless Network</a> .....	46
<a href="#">Configuring LAN Ports</a> .....	48

## Configuring Device Settings

Device settings refer to the device name and service provider login settings.

Figure 16. The Configuration :: Device page

The screenshot displays the 'Configuration :: Device' page for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page is divided into a left sidebar with navigation links (Status, Configuration, Maintenance, Administration) and a main content area. The main content area contains the following sections:

- Device Information:** Fields for Device Name (RuckusAP), Device Location, and GPS Coordinates (e.g., 37.388, -122.0258633).
- Service Provider Login:** Fields for Username (super), Current Password, New Password, and Confirm New Password.
- Buttons:** 'Update Settings' and 'Restore previous settings'.

The footer of the page includes the Ruckus logo and the text 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' and '© Copyright 2009 Ruckus Wireless'.

### To configure the device settings

1. Go to **Configuration > Device**. The Configuration :: Device page appears.
2. In **Device Name**, type a new name for the device or leave as is to accept the default device name (RuckusAP). The device name identifies the Multimedia Wi-Fi Wall Switch among other devices on the network.
3. Under **Service Provider Login**, change the login information as required:
  - **Username:** Type the name that you want to use for logging into the Web interface. The default user name is super.
  - **Password:** Type the new password that you want to use. The password must consist of six to 32 alphanumeric characters only.
  - **Password confirmation:** Retype the new password to confirm.
4. Click **Update Settings** to save and apply your changes.

## Configuring Internet Settings

Internet settings define how the Multimedia Wi-Fi Wall Switch connects to your local area network and to the Internet. This section describes how to view and configure the Multimedia Wi-Fi Wall Switch's Internet settings. Topics discussed include:

- [Default IP Addressing Behavior](#)
- [Obtaining and Assigning an IP Address](#)
- [Changing the Network Connection Type](#)
- [Renewing and Releasing DHCP](#)

### Default IP Addressing Behavior

By default, the Multimedia Wi-Fi Wall Switch is configured to automatically obtain an IP address from a DHCP server on the network. If the Multimedia Wi-Fi Wall Switch does not detect a DHCP server, it automatically assigns itself the static IP address 192.168.0.1 to make it easier for you to preconfigure and deploy it your network.

### Obtaining and Assigning an IP Address

There are at least two instances when you would want to change the IP address of the Multimedia Wi-Fi Wall Switch:

- If the current IP address that the Multimedia Wi-Fi Wall Switch is using consistently conflicts with that of another device on the network
- If you want to switch from DHCP to static IP addressing, for use in managing or maintaining the Multimedia Wi-Fi Wall Switch

Unless you are able to determine the IP address assigned by the DHCP server to the Multimedia Wi-Fi Wall Switch, it may prove helpful for anyone needing administrative access to assign a static IP address to Access Point.

Figure 17. The Configuration :: Internet page

The screenshot shows the web interface for configuring a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page title is "Configuration :: Internet". On the left is a navigation menu with sections: Status (Device, Internet, Wireless), Configuration (Device, Internet, Wireless, LAN Ports), Maintenance (Upgrade, Reboot / Reset, Support Info), and Administration (Management, Diagnostics). The "Internet" option under "Configuration" is selected. The main content area contains fields for "Primary DNS Server", "Secondary DNS Server", and "NTP Server" (pre-filled with "ntp.ruckuswireless.com"). Below these is the "Connection Type" section with radio buttons for "DHCP" (selected) and "Static IP". At the bottom of the form are buttons for "Update Settings" and "Restore previous settings". A "Need Help?" button is in the top right. The footer includes the Ruckus logo and the text "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" and "© Copyright 2009 Ruckus Wireless".

#### To assign a static IP address to the AP

1. Go to **Configuration > Internet**. The Internet page appears.
2. Verify that **Connection Type** is set to **Static IP**.
3. When the Static IP options appear, you can changes to the following settings:
  - **Gateway**: This is the gateway IP address of the Internet interface.
  - **Primary DNS Server**: The IP address of the primary Domain Name System (DNS) server.
  - **Secondary DNS Server**: The IP address of the secondary Domain Name System (DNS) server.
  - **NTP Server**: Hostname of the Network Time Protocol (NTP) server.
4. Click **Update Settings** to save your changes.

## Changing the Network Connection Type

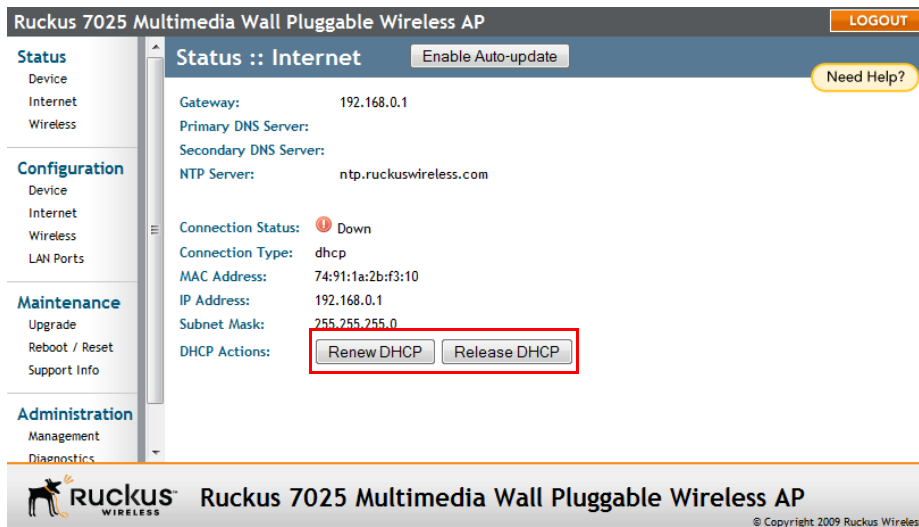
To change the connection type (DHCP or Static IP)

1. Go to **Configuration > Internet**. The Configuration > Internet page appears.
2. In *Connection Type*, select **DHCP** or **Static IP**.
3. If you selected **Static IP**, fill in the related fields according to your network configuration:
  - **Gateway**: This is the gateway IP address of the Internet interface.
  - **Primary DNS Server**: The IP address of the primary Domain Name System (DNS) server.
  - **Secondary DNS Server**: The IP address of the secondary Domain Name System (DNS) server.
  - **NTP Server**: Hostname of the Network Time Protocol (NTP) server.
4. Under *Home Connection Settings*, enter the **IP Address** and **Subnet Mask** for the AP.
5. Click **Update Settings** to save your changes.

## Renewing and Releasing DHCP

This task should be performed only if you have access to the DHCP server or have some way to determine what IP address has been assigned to the AP. It serves as a troubleshooting technique when IP addresses to one or more networked devices prove to be unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

Figure 18. Renew or Release DHCP



**To renew or release the DHCP server-assigned IP address**

1. Go to **Status > Internet**.
2. Review the current settings.
3. If the current **Connection Type** is **DHCP**, you will be able to see the currently-assigned IP address and subnet mask listed below.
  - To force the DHCP server to assign a new IP address to the Multimedia Wi-Fi Wall Switch, click **Renew DHCP**. If the AP is listed in the DHCP server's address table, it will attempt to reassign the previous address to the AP (unless the address is already in use).
  - To force the DHCP server to assign a new IP addresses to all networked devices at the same time (including this Access Point), click **Release DHCP**. This will cause a temporary interruption in overall network service.
4. Click **Update Settings** to save your settings.



## Configuring Wireless Settings

This section describes how to configure the wireless settings of the ZF7025 Multimedia Wi-Fi Wall Switch. There are two types of wireless settings that you need to configure:

- [Configuring Common Wireless Settings](#): Includes the wireless mode, country code, and advanced wireless settings, such as the wireless transmit power and wireless protection mode.
- [Configuring Wireless # Settings](#): Includes settings that allow wireless clients on your network to connect to the Multimedia Wi-Fi Wall Switch.

Refer to the sections below for instructions on how to configure each set of wireless settings.

## Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. These settings include the wireless channel, channel width and country code.

Figure 19. The Configuration :: Wireless page

The screenshot displays the web interface for configuring the Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page title is "Configuration :: Wireless :: Common". The left sidebar contains navigation menus for Status, Configuration, Maintenance, and Administration. The main content area shows settings for Wireless Mode (2.4GHz (802.11b/g/n)), Channel (SmartSelect), Channel Width (20 MHz), and Country Code (United States). There is an "Advanced Settings" section with a radio button for "AeroScout RFID tag detection" set to "Disabled". At the bottom, there are "Update Settings" and "Restore previous settings" buttons. The footer includes the Ruckus logo and copyright information.

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

LOGOUT

Configuration :: Wireless :: Common

Common Wireless 1 Wireless 2 Wireless 3 Wireless 4 Wireless 5 Wireless 6 Wireless 7 Need Help?

Wireless Mode: 2.4GHz (802.11b/g/n)

Channel: SmartSelect

Channel Width: 20 MHz

Country Code: United States

Advanced Settings: Edit Common Settings

AeroScout RFID

AeroScout RFID tag detection: ☒ Disabled ☐ Enabled

Update Settings Restore previous settings

Ruckus WIRELESS Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

### To configure the wireless settings common to all WLANs

1. Go to **Configuration > Wireless**. The Configuration :: Wireless :: Common page appears.
2. Make changes to the common wireless settings listed in the table below.

Table 12. Common Wireless settings

Setting	Description
Wireless Mode	Only one wireless mode is available on the ZF7025: <ul style="list-style-type: none"><li>• <b>2.4GHz (802.11b/g/n)</b>: This setting allows 802.11b, 802.11g, and 802.11n compliant devices to join the network on the 2.4GHz unlicensed band.</li></ul>
Channel	This option lets you select the channel used by the network. You can choose SmartSelect, or choose one of a specific number of channels. If you choose <b>SmartSelect</b> , the AP automatically selects the best channel (encountering the least interference) to transmit the signal.
Channel Width	Set Channel Width to 40Mhz or 20Mhz (default). The 802.11n standard allows the use of 40MHz channel width, which allows higher transmission speeds. Setting the channel width to 20MHz will result in lower transmission speeds, but can allow for more wireless devices to be deployed in proximity without overlapping channels.
Country Code	This option (if enabled) lets you select your country or region code.
Advanced Settings	Refer to <a href="#">“Reviewing Common Advanced Settings”</a> on <a href="#">page 33</a> .
AeroScout RFID	Select <b>Enabled</b> to enable AeroScout RFID tag detection.



**CAUTION:** Selecting the incorrect country or region may result in violation of applicable laws. If you purchased the Multimedia Wi-Fi Wall Switch in the United States, you do not need to set the country code manually. Ruckus Wireless devices that are sold in the US are preconfigured with the correct country code and this setting is non-configurable.

3. If you are using AeroScout Tags in your organization to locate assets or personnel, you can use your ZoneFlex AP to relay location or presence data from the AeroScout Tags to the AeroScout Engine via Wi-Fi.

To enable the AP to relay AeroScout data, click the **Enable** option in **AeroScout-RFID tag detection**.

To check the status of the AeroScout communication agent (which relays location data from AeroScout Tags to the AeroScout Engine), go to the **Status > Wireless** page. Refer to ["Viewing Current Wireless Settings"](#) on [page 52](#) for more information.



**NOTE:** For other AeroScout-related configuration, refer to the AeroScout documentation that was shipped with your AeroScout Tag and AeroScout Engine.

---



**NOTE:** If ZoneDirector exists on the network, you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for more information.

---

4. Click **Update Settings** to save your settings.

## Reviewing Common Advanced Settings

Advanced wireless settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.



**CAUTION:** To fully benefit from the Multimedia Wi-Fi Wall Switch's capabilities, it is advisable not to change these values unless absolutely necessary.

---

Figure 20. The Configuration :: Wireless :: Advanced :: Common page

The screenshot shows the web interface of a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The top header bar is dark grey with the text 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' on the left and a 'LOGOUT' button on the right. Below this is a blue navigation bar with the text 'Configuration :: Wireless :: Advanced :: Common' and a 'Need Help?' button. On the left side, there is a vertical sidebar menu with sections: 'Status' (Device, Internet, Wireless), 'Configuration' (Device, Internet, Wireless, LAN Ports), 'Maintenance' (Upgrade, Reboot / Reset, Support Info), and 'Administration' (Management, Diagnostics). The main content area has a white background. It contains a 'Transmit Power' dropdown menu set to 'Full', a 'Protection Mode' section with three radio buttons ('Disabled' is selected, followed by 'CTS-only' and 'RTS-CTS'), an 'Update Settings' button, and a link 'Restore previous settings'. Below these is a link that says 'Go back to Wireless Configuration'. At the bottom of the page is a grey footer bar with the Ruckus logo on the left, the text 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' in the center, and '© Copyright 2009 Ruckus Wireless' on the right.

**To configure the advanced common options**

1. On the **Configuration > Wireless** page, click **Edit Common Settings**. The *Configuration :: Wireless :: Advanced :: Common* page appears.

2. Configure the advanced settings listed in [Table 13](#) as required.

Table 13. *Advanced > Common options*

Option	Description
Transmit Power	The default setting is <b>Full</b> . Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the predefined power (this value differs according to the current country code).
Protection Mode	<p>(Inactive by default.) If you activate protection, you control how 802.11 devices know when they should communicate to another device. This is important in a mixed environment of both 802.11b and 802.11g clients.</p> <p><i>WARNING: Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g devices but will severely decrease performance.</i></p> <ul style="list-style-type: none"><li>• <b>CTS-only</b>: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.</li><li>• <b>RTS/CTS</b>: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.</li></ul>

3. Click **Update Settings** to save and apply the changes.

## Configuring Wireless # Settings

The ZF7025 provides up to eight wireless LANs that can be individually configured to provide different kinds of services for different kinds of wireless clients, traffic types or different user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.

Figure 21. Wireless # settings

The screenshot shows the web interface for configuring a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page title is "Configuration :: Wireless :: Wireless 1". The left sidebar contains navigation menus for Status, Configuration, Maintenance, and Administration. The main content area has tabs for Common, Wireless 1, Wireless 2, Wireless 3, Wireless 4, Wireless 5, Wireless 6, and Wireless 7. The "Wireless 1" tab is selected. The configuration options include: Wireless Network (set to Wireless 1), Wireless Availability? (radio buttons for Enabled and Disabled, with Enabled selected), Broadcast SSID? (radio buttons for Enabled and Disabled, with Enabled selected), SSID (text field containing Wireless1), Threshold Settings (button Edit Settings), Rate Limiting (button Edit Settings), Access Control (button Edit Settings), VLAN (radio buttons for No VLAN and VLAN ID, with No VLAN selected), and Encryption Method (dropdown menu set to Disabled). At the bottom, there are buttons for Update Settings and Restore previous settings. The footer includes the Ruckus logo and copyright information: © Copyright 2009 Ruckus Wireless.

### To configure wireless settings

1. Go to **Configuration > Wireless**. The *Configuration :: Wireless :: Common* page appears.
2. Click one of the two **Wireless (#)** tabs. The *Configuration :: Wireless :: Wireless [#]* page appears.
3. Review the WLAN options listed in [Table 14](#), and then make changes as required.

Table 14. Wireless [#] options

Option	Description
Wireless Network	This wireless network name is for management purposes only, and is not visible to the user.
Wireless Availability	This option controls whether or not the wireless network is available to users (Off or On).
Broadcast SSID	This option controls whether or not the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user must be told the correct SSID before they can connect to your network.

Table 14. Wireless [#] options

SSID	This is the publicly-broadcast “name” of your wireless network. SSIDs can contain up to 32 alphanumeric characters and are case-sensitive.
Dynamic VLAN	This allows the RADIUS server to indicate the virtual LAN assignment of a wireless client during the 802.1X authentication process.
Threshold Settings	<p>This button opens a page where you can configure the Protection Mode you activated on the <i>Configuration :: Wireless :: Advanced :: Wireless [#]</i> page. If Protection Mode is not active, ignore this option.</p> <p>For more information, see <a href="#">“Setting Threshold Options”</a> on <a href="#">page 43</a>.</p>
Rate Limiting	This button opens a page where you can configure upload and download limits per station. For more information, see <a href="#">“Rate Limiting”</a> on <a href="#">page 45</a> .
Access Control	This button opens a page where you can configure access controls for the WLAN. For more information, see <a href="#">“Controlling Access to the Wireless Network”</a> on <a href="#">page 46</a> .
VLAN	Enable this option and enter a VLAN ID if you want to tag all traffic from this WLAN to a specific VLAN.
Encryption Method	<p>By default, all data exchanges on your wireless network are not encrypted, but you can pick an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings.</p> <p>Ruckus Wireless strongly recommends using WPA encryption, as WEP has been proven to be easily circumvented.</p> <p>For more information, see either <a href="#">“Using WEP”</a> on <a href="#">page 38</a> or <a href="#">“Using WPA”</a> on <a href="#">page 40</a>.</p>

4. When you are finished, click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
5. Click **Go back to Wireless Configuration** to reopen the previous page.

## Using WEP



**CAUTION:** WEP encryption has been proven to be easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.



**CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

Figure 22. WEP settings

The screenshot shows the configuration page for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The left sidebar contains navigation links: Status (Device, Internet, Wireless), Configuration (Device, Internet, Wireless, LAN Ports), Maintenance (Upgrade, Reboot / Reset, Support Info), and Administration (Management, Diagnostics, Log). The main content area is titled 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' and includes a 'LOGOUT' button. The 'Wireless' section is active, showing various settings. Under 'Threshold Settings', 'Rate Limiting', and 'Access Control', there are 'Edit Settings' buttons. The 'VLAN' section has radio buttons for 'No VLAN' (selected) and 'VLAN ID' with an input field. The 'Encryption Method' is set to 'WEP', with a red box highlighting the warning: '\*\* 11n performance not available with WEP encryption \*\*'. The 'Authentication Mode' has radio buttons for 'Open', 'Shared Key' (selected), and 'Auto'. The 'Encryption Strength' is set to '64 bit (10 hex digits/ 5 ASCII keys)'. The 'Key Entry Method' has radio buttons for 'Hexadecimal' (selected) and 'ASCII Text'. The 'Passphrase' field is empty, with a 'Generate' button next to it. The 'WEP Key' field contains '3A5401F51B'. The 'Key Index' is set to '1'. At the bottom, there are 'Update Settings' and 'Restore previous settings' buttons. The footer includes the Ruckus logo and the text 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' and '© Copyright 2009 Ruckus Wireless'.

### To configure WLAN-specific WEP encryption settings

1. Go to **Configuration > Wireless**. The Configuration :: Wireless :: Common page appears.
2. Click the **Wireless #** tab that you want to configure. The Configuration :: Wireless :: Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WEP**. An additional set of WEP-specific encryption options appear on this page.



4. Review the encryption settings listed in [Table 15](#), and then make changes as required.

Table 15. WEP settings

Encryption Setting	Description
Authentication Mode	<p>Your options include:</p> <ul style="list-style-type: none"> <li>• Open: No security measure is enforced.</li> <li>• Shared Key: The selected Default Shared Key is used.</li> <li>• Auto: Automatically-selected authentication mode.</li> </ul>
Encryption Strength	<ul style="list-style-type: none"> <li>• 64 bit: Specify the key with 10 hexadecimal digits or 5 ASCII characters.</li> <li>• 128 bit: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.</li> </ul>
Key Entry Method	<ul style="list-style-type: none"> <li>• Hexadecimal: The encryption key only accepts hexadecimal characters (0-9, A-F).</li> <li>• ASCII Text: The encryption key accepts ASCII characters.</li> </ul>
Passphrase	<p>This assists in automatic key generation. Enter some text and click the <b>Generate</b> button. The system will generate the WEP key automatically. You may specify a passphrase up to 32 characters.</p> <p>Please note that the algorithm used for key generation may vary from system to system. Checking the WEP keys used between wireless stations and the Multimedia Wi-Fi Wall Switch is recommended.</p>
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from "1" to "4", that the WEP key is to be stored in.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.
6. Click **Go back to Wireless Configuration** to reopen the previous page.

## Using WPA

Use of WPA-PSK allows automatic key generation based on a single passphrase. WPA-PSK provides very strong security, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the WLAN with WPA-PSK, some network users will not be able to connect to your WLAN unless their devices are manually set to WPA-PSK and configured with the same passphrase.

Figure 23. WPA settings

The screenshot displays the configuration interface for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page is titled "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" and includes a "LOGOUT" button in the top right corner. A left-hand navigation menu is organized into four sections: "Status" (Device, Internet, Wireless), "Configuration" (Device, Internet, Wireless, LAN Ports), "Maintenance" (Upgrade, Reboot / Reset, Support Info), and "Administration" (Management, Diagnostics, Log). The "Wireless" tab under the "Configuration" section is selected. The main content area shows settings for "Wireless Network: Wireless 1". Key settings include "Wireless Availability?" (Enabled), "Broadcast SSID?" (Enabled), "SSID:" (ruckus AP), and "Threshold Settings:" (with Edit Settings buttons for Rate Limiting and Access Control). The "VLAN:" section is set to "No VLAN". The "Encryption Method:" is set to "WPA", which has expanded to show "WPA Version:" (WPA2 selected), "WPA Authentication:" (PSK selected), and "WPA Algorithm:" (AES selected). A "Passphrase:" field contains "a passphrase". At the bottom of the settings area are "Update Settings" and "Restore previous settings" buttons. The footer features the Ruckus logo and the text "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" and "© Copyright 2009 Ruckus Wireless".

### To configure WPA encryption settings

1. Go to **Configuration > Wireless**. The Configuration :: Wireless :: Common page appears.
2. Click the Wireless # tab that you want to configure. The Configuration :: Wireless :: Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WPA**. An additional set of WPA-specific encryption options appear on this page.

4. Review the encryption settings listed in [Table 16](#), and then make changes as preferred.

Table 16. WPA settings

Encryption Setting	Description
WPA Version	<p>Your options are WPA, WPA2 or WPA Auto.</p> <ul style="list-style-type: none"> <li>When <b>WPA</b> is selected, the wireless client decides which version of WPA will be used. WPA is the recommended default for best compatibility. Wi-Fi WPA-capable PDAs and other devices are usually limited to WPA + TKIP.</li> <li><b>WPA2</b> is an advanced option. WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later.</li> <li><b>WPA-Auto</b> is an advanced option. Only the best WPA 802.11i conforming/Wi-Fi WPA-certified client devices can operate in this mode.</li> </ul>
WPA Authentication	<p><b>PSK</b> mode is suitable for home or personal use. <b>802.1X</b> mode uses a RADIUS server to verify user identity. The auto mode offers both options for the wireless client to pick.</p> <p>For more information on how to configure the 802.1X mode, refer to "<a href="#">Customizing 802.1X Settings</a>" on <a href="#">page 42</a>.</p>
WPA Algorithm	<p>When <b>Auto</b> is selected, the wireless client decides whether <b>TKIP</b> or <b>AES</b> will be used. AES is the strongest encryption and requires additional hardware support on wireless devices. Auto is an advanced option and some wireless clients may fail to associate.</p>
Passphrase	<p>Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).</p>

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.
6. Click **Go back to Wireless Configuration** to reopen the previous page.

## Customizing 802.1X Settings



**CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

If you choose WPA as the encryption method, you have the option to set up the Multimedia Wi-Fi Wall Switch to act as an 802.1X proxy, utilizing external authentication sources such as a RADIUS server. This provides a higher level of security, when compared to the static security process in a WEP configuration.

Using 802.1X lets a device complete authentication prior to the exchange of data, as in a DHCP environment. Another benefit is that each BSSID can be individually configured to forward all authentication requests to its own server.

Figure 24. 802.1X settings

The screenshot shows the configuration interface for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page has a sidebar on the left with sections: Status (Device, Internet, Wireless), Configuration (Device, Internet, Wireless, LAN Ports), Maintenance (Upgrade, Reboot / Reset, Support Info), and Administration (Management, Diagnostics, Log). The main content area is titled 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' and includes a 'LOGOUT' button. The 'Wireless' configuration section is active, showing 'Encryption Method' set to 'WPA'. Under 'WPA Version', 'WPA2' is selected. Under 'WPA Authentication', '802.1x' is selected. Under 'WPA Algorithm', 'AES' is selected. The 'Radius NAS-ID' field is empty. The 'Authentication Server' section is marked '\*\* Required \*\*' and includes fields for 'IP address', 'Port', and 'Server Secret'. The 'Accounting Server' section is marked '\*\* Optional \*\*' and includes fields for 'IP address', 'Port', and 'Server Secret'. At the bottom, there are buttons for 'Update Settings' and 'Restore previous settings'. The footer shows the Ruckus logo and copyright information: '© Copyright 2009 Ruckus Wireless'.

### To configure WLAN-specific 802.1X authentication settings

1. Go to **Configuration > Wireless**. The Configuration :: Wireless :: Common page appears.
2. Click a **Wireless #** tab to configure. The Configuration :: Wireless :: Wireless[#] page appears.
3. Click the **Encryption Method** menu, then click **WPA**. The basic set of WPA-specific encryption options appear on the page.
4. Select **802.1X** as the WPA Authentication mode. Additional options appear.
5. Configure the following settings to customize your 802.1X authentication:

- **RADIUS NAS-ID:** Enter the network ID assigned to your RADIUS server.
  - **Authentication Server [-Required-]:** Enter the information needed to establish a connection between the Multimedia Wi-Fi Wall Switch and the RADIUS server.
  - **Accounting Server [-Optional-]:** Enter the information needed to establish this connection.
6. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
  7. Click **Go back to Wireless Configuration** to reopen the previous page.

## Setting Threshold Options

The following options allow you to fine-tune the “Protection Mode” behavior, set previously on the *Configuration :: Wireless :: Advanced :: Common* page. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, which determine what is put into effect and when.



---

**CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

---

### To customize Protection Mode (Threshold) settings

1. Go to **Configuration > Wireless**. The *Configuration :: Wireless :: Common* page appears.
2. Click the tab for the Wireless # (WLAN) that you want to configure. The *Configuration :: Wireless :: Wireless [#]* page appears.
3. Look for **Threshold Settings**, and then click **Edit Settings**. The *Configuration :: Wireless :: Advanced :: Wireless [#]* page appears.

4. Review the options listed in [Table 17](#), and then make any needed changes.

Table 17. Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in milliseconds. A beacon is a broadcast packet sent by the AP to synchronize the wireless network.
Data Beacon Rate	(The default value is 10.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.
RTS/CTS Threshold	(The default value is 2346.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in an environment with excessive signal noise or hidden nodes, but may result in some performance degradation.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

You have completed configuring the threshold options. To reopen the previous page, click the **Go back to Wireless Configuration** link.

Figure 25. Threshold settings

The screenshot displays the web interface for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page title is "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" with a "LOGOUT" button in the top right. The left sidebar contains navigation menus: "Status" (Device, Internet, Wireless), "Configuration" (Device, Internet, Wireless, LAN Ports), "Maintenance" (Upgrade, Reboot / Reset, Support Info), and "Administration" (Management, Diagnostics, Log). The main content area is titled "Configuration :: Wireless :: Advanced :: Wireless 1" and includes a "Need Help?" button. It features three input fields: "Beacon Interval" set to 100 (range 100,200...1000), "Data Beacon Rate (DTIM)" set to 1 (range 1 - 255), and "RTS / CTS Threshold" set to 2346 (range 256 - 65535). Below these fields are buttons for "Update Settings" and "Restore previous settings", and a link to "Go back to Wireless Configuration". The footer shows the Ruckus logo and "© Copyright 2009 Ruckus Wireless".

## Rate Limiting

Rate Limiting allows you to cap the data transfer rates per client for a specific WLAN.

### To enable per station rate limits

1. Go to **Configuration > Wireless**.
2. Select the WLAN that you want to configure from the tabs at the top of the page.
3. Click the **Edit Settings** button next to *Rate Limiting*. The *Rate Limiting* page appears.
4. Set the maximum **Downlink** and **Uplink** rate per station, or leave disabled if you do not want to limit traffic rate per station in that direction.
5. The table below updates to show the maximum transfer rates for each traffic type.
6. Click **Update Settings** to save your changes.

Figure 26. Limit per station traffic rates on a specific WLAN

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

Configuration :: Wireless :: Advanced Wireless Rate Limiting :: Wireless 1

Per Station Traffic Rate: Downlink: 500 kbps link per station Uplink: 100 kbps link per station

Maximum traffic rate on per station basis

Class	Downlink / Uplink		
	Rate (kbps)	Ceiling (kbps)	Buffer (pkts)
Voice	100 / 25	128 / 100	10 / 5
Video	100 / 25	400 / 100	25 / 5
Best-Effort	200 / 25	500 / 100	25 / 5
Background	100 / 25	500 / 100	10 / 5

Update Settings Restore previous settings

- Go back to Wireless Configuration

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

## Controlling Access to the Wireless Network

Access Control enables you to specify the stations are allowed to join (associate with) your WLAN networks. Access controls can be configured for each WLAN from its respective *Wireless #* tab.

### Access Control Options

This section describes the options that you can use to control access to the wireless network.

- **Disabling WLAN Access Restrictions:** If you select **Disable WLAN access restrictions**, then MAC-address-based restrictions on which stations can join the WLAN are disabled; thus, any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption passphrase. The Access Controls table is hidden if the current mode is **Disable WLAN access restrictions**.
- **Allowing Only Stations Listed in the Access Controls Table:** If you select **Allow only stations listed in the Access Controls Table**, then stations entered into the access-controls table are allowed but all others are disallowed. To add MAC addresses, see [“Changing the Access Controls for a WLAN”](#) on [page 47](#).



- **Denying Only Stations Listed in the Access Controls Table:** If you select **Deny only stations listed in the Access Controls Table**, then stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see [“Changing the Access Controls for a WLAN”](#) on [page 47](#).

## Changing the Access Controls for a WLAN

By default, the **Disable WLAN access restrictions** option is selected, which allows any wireless station to gain access to the wireless network. If you want to change this setting, follow the instructions below.

Figure 27. Access control settings

The screenshot shows the configuration interface for a Ruckus 7025 Multimedia Wall Pluggable Wireless AP. The page title is "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" with a "LOGOUT" button. The left sidebar contains navigation menus: "Status" (Device, Internet, Wireless), "Configuration" (Device, Internet, Wireless, LAN Ports), "Maintenance" (Upgrade, Reboot / Reset, Support Info), and "Administration" (Management, Diagnostics, Log). The main content area is titled "Configuration :: Wireless :: Access Control :: Wireless 1" and includes a "Need Help?" button. It features three radio buttons for access control: "Disable WLAN access restrictions", "Allow only stations listed in the Access Control Table", and "Deny only stations listed in the Access Control Table" (which is selected). Below these is the "Access Control Table" with columns for "Address" and "Remove?". Two rows of MAC address input fields are shown, each with a "Cancel" button. An "Add new entry" button is at the bottom left of the table. Below the table are "Update" and "Restore previous settings" buttons. A link at the bottom says "Go back to Wireless Configuration". The footer includes the Ruckus logo and "Ruckus 7025 Multimedia Wall Pluggable Wireless AP" with a copyright notice "© Copyright 2009 Ruckus Wireless".

### To edit the ACL

1. Go to **Configuration > Wireless**.
2. Click the **Wireless #** tab for which you want to configure the access control settings.
3. Click the **Edit Settings** button next to *Access Control*.
4. Select the radio button for the desired access control. (For a description of the options, see [“Access Control Options”](#) in the previous section.) The Access Controls Table appears.
5. To add a MAC address to the Access Control table, click the **Add new entry** button.
6. Fill out the following text boxes:

- **Address:** Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. You can specify a full 12-hex-digit MAC address or enter "wildcard" characters for "don't care" digits. Allowable hex-digit characters are 0-9, a-f, and A-F. Most address-tags and software where you find MAC addresses listed include colons or dashes to separate the address-pairs; that is provided for you on the web page, so do not enter the colons or dashes.

Supported wildcard characters include "x", "X" and blank (space character). Wildcards are useful when you want to specify all MAC addresses from a given manufacturer. For example, by specifying only the Organizationally Unique Identifier (the first six hexadecimal digits of any MAC address from that manufacturer is its OUI) saves you having to enter all 24 million of them (the table size is limited in the AP/Router to 128 entries). Some manufacturers produce devices using more than one OUI, in which case you may need to enter each applicable one.

7. Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row will be added to the table.

You have completed adding an entry to the MAC address table. If you have additional MAC addresses you want included, click **Add new entry**, and then repeat these steps until you have entered all the stations you want. There is a limit of 128 rows.

## Removing a MAC Address

To remove a MAC address from the ACL table, click the **Cancel** button under the *Remove* column, and then click **Update**. The ACL table refreshes, and the MAC address that you deleted disappears from the table.

## Configuring LAN Ports

Each of the four LAN ports on the bottom of the AP can be configured independently, allowing you to disable one or more ports or assign a VLAN ID to each port.

By default, the LAN1-LAN4 ports are enabled Access Ports with no VLAN assigned. The LAN5/Uplink port on the rear of the ZF7025 is a trunk port and is not configurable.

LAN4 also provides PoE out to provide power to PoE-capable devices such as IP phones. Additionally, the ZF7025 includes a pass through port on the side. The pass through port is not configurable.

Figure 28. The Configuration :: LAN Ports page

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

LOGOUT

Status

Device

Internet

Wireless

Configuration

Device

Internet

Wireless

LAN Ports

Maintenance

Upgrade

Reboot / Reset

Support Info

Administration

Management

Diagnostics

Log

Configure :: LAN Ports

Need Help?

LAN1 Port

☒ Enable

No VLAN

VLAN ID

Access Port

LAN2 Port

☒ Enable

No VLAN

VLAN ID

Access Port

LAN3 Port

☒ Enable

No VLAN

VLAN ID

Access Port

LAN4 Port


☒ Enable


No VLAN

VLAN ID

Access Port

Update Settings



 Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

To configure LAN ports

- Go to **Configuration > LAN Ports**.
- Review the following table and make changes as needed for each of the ports labeled **LAN 1** through **LAN 4**, which correspond to the labels on the outside of the AP.

Table 18. Configure the LAN ports

Setting	Description
Enable	All LAN ports are enabled by default. Unchecking this box next to a port disables that LAN port entirely. If you do not want to provide wired access through the AP, uncheck (clear) the <b>Enable</b> box next to each LAN port.
No VLAN	Selecting <b>No VLAN</b> disables VLAN tagging on the access port.
VLAN ID	Selecting <b>VLAN ID</b> and entering a VLAN ID number in the field segments all traffic arriving into this LAN port into the VLAN specified. Valid entries are 2-4094.

- Click **Update Settings** to save your changes.

## Working with Port-Based VLANs

The ZoneFlex 7025 Multimedia Wi-Fi Wall Switch provides options for segmenting all incoming traffic (both wireless and wired Ethernet traffic) into specific VLANs. There are three ways to segment incoming traffic into VLANs:

- Each of the eight wireless interfaces (SSIDs) can be configured with a specific VLAN ID: (**Configuration > Wireless > Wireless [#] > VLAN**).
- Each of the eight wireless interfaces (SSIDs) can be configured with Dynamic VLAN if 802.1X authentication with a RADIUS server is configured (**Configuration > Wireless > Wireless [#] > Dynamic VLAN**).
- Each of the four front-facing LAN ports can be configured with a specific VLAN ID (**Configure > LAN Ports > VLAN ID**).

# Managing the Multimedia Wi-Fi Wall Switch

## In This Chapter

<a href="#">Viewing Current Wireless Settings</a> .....	52
<a href="#">Changing the Administrative Login Settings</a> .....	53
<a href="#">Configuring Management Access Options</a> .....	55
<a href="#">Sending a Copy of the Log File to Ruckus Wireless Support</a> .....	58
<a href="#">Enabling Logging and Sending Event Logs to a Syslog Server</a> .....	57
<a href="#">Upgrading the Firmware</a> .....	59
<a href="#">Rebooting the Multimedia Wi-Fi Wall Switch</a> .....	63
<a href="#">Resetting to Factory Defaults</a> .....	64
<a href="#">Running Diagnostics</a> .....	64

## Viewing Current Wireless Settings

If you want to view the current common wireless settings that the Multimedia Wi-Fi Wall Switch is using, go to the **Status > Wireless** page. [Table 19](#) lists the descriptions of each common wireless setting.

Figure 29. The Status > Wireless page

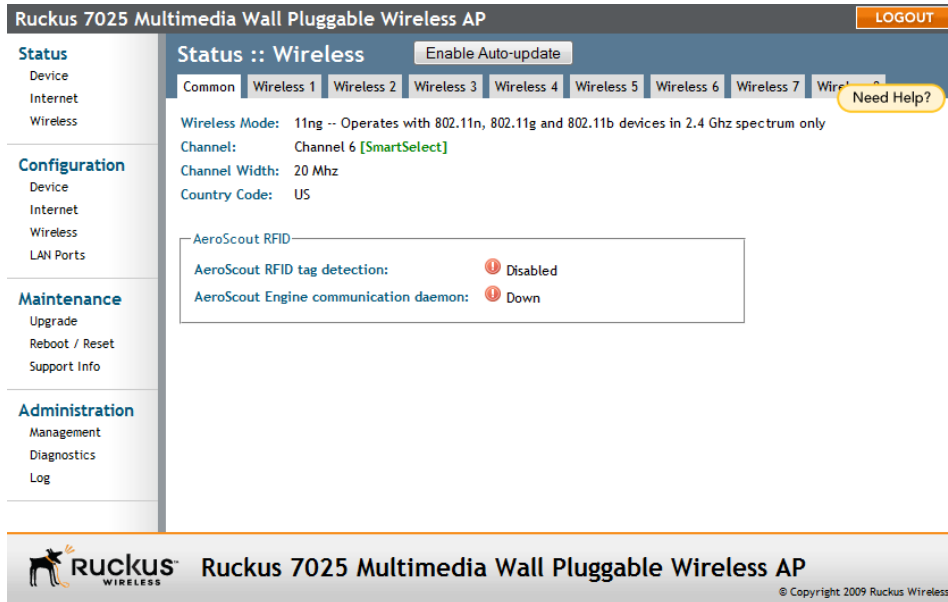


Table 19. Common Wireless settings

Setting	Description
Wireless Mode	Shows the wireless mode that the Multimedia Wi-Fi Wall Switch is currently using. Possible values include: <ul style="list-style-type: none"><li>• 11n/g</li></ul>
Channel	Shows the wireless channel that the Multimedia Wi-Fi Wall Switch is currently using. If you set the wireless channel to SmartSelect, this field will show the value <b>Channel # [SmartSelect]</b> .
Channel Width	Shows the current channel width (20MHz or 40MHz).
Country Code	Shows the country code that the Multimedia Wi-Fi Wall Switch has been set to use.  <i>CAUTION: Verify that the Multimedia Wi-Fi Wall Switch is using the correct country code to make sure it uses only the allowed radio channels in your region. Selecting the incorrect country code may result in violation of application laws.</i>
AeroScout RFID tag detection	Shows <b>Enabled</b> if you enabled AeroScout RFID tag detection. The default setting is <b>Disabled</b> .
AeroScout Engine communication daemon	Shows <b>Up</b> if the communication agent on the AP is able to relay location data from AeroScout Tags to the AeroScout Engine. If the communication agent is unable to relay data or AeroScout tag detection is disabled, this field will show <b>Down</b> .

If you want to make changes to any of these settings, go to the **Configuration > Wireless** page. Refer to [“Configuring Common Wireless Settings”](#) on [page 31](#) for more information.

## Changing the Administrative Login Settings

The default user name is `super` and the default password is `sp-admin`. To prevent unauthorized users from logging in to the Web interface using these default administrator login settings, Ruckus Wireless recommends that you change the default Web interface password immediately after your first login.

### To change the default administrator login settings

1. Log into the Web interface.
2. Go to **Configuration > Device**. The Device page appears.

3. Under **Service Provider Login**, change the default administrator login settings.
  - (Optional) In **Username**, type a new user name that you will use to log in to the Web interface. The default user name is `super`.
  - In **Password**, type a new password to replace the default password `sp-admin`.
  - In **Password Confirmation**, retype the new password.
4. Click **Update Settings**. The message *Your parameters were saved* appears.

You have completed changing the default login settings. The next time you log in to the Web interface, make sure you use these updated login settings.

Figure 30. The Configuration > Device page

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

LOGOUT

Configuration :: Device

Need Help?

Device Name:

Device Location:

GPS Coordinates:  ,  (e.g. 37.388, -122.0258633)

**Service Provider Login**

Username:

Current Password:

New Password:

Confirm New Password:

[Restore previous settings](#)

Ruckus WIRELESS Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

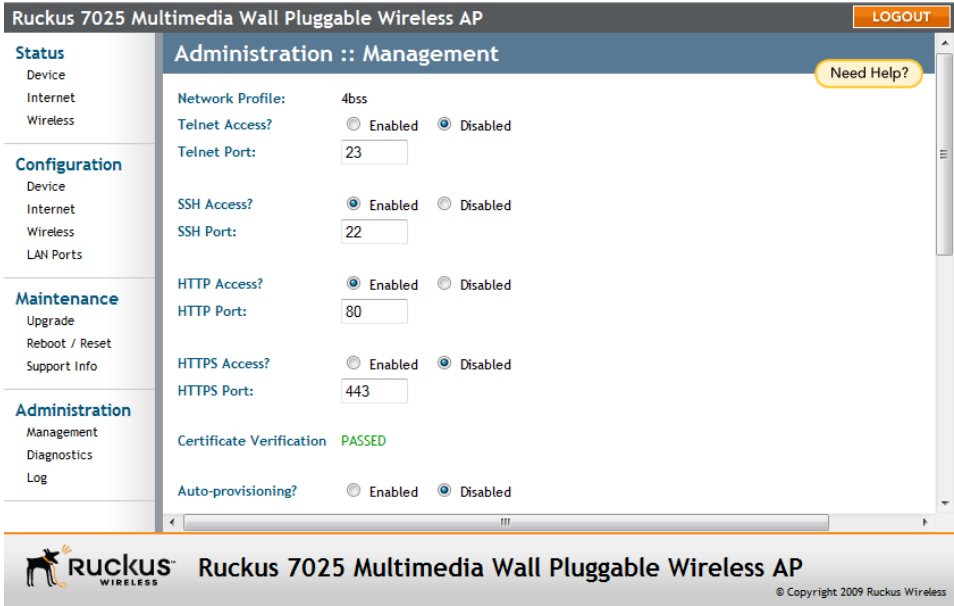


# Configuring Management Access Options

In addition to managing the Multimedia Wi-Fi Wall Switch via a Web browser through HTTP, several other management access options are available on the AP. These options include management access via HTTPS, Telnet, and SSH.

You can also enable remote management, if you want to be able to access the Multimedia Wi-Fi Wall Switch Web interface from outside your local network.

Figure 31. The Administration > Management page



## To configure management access options

1. Go to **Administration > Management**. The Management page appears.

2. Review the access options listed in [Table 20](#), and then make changes as needed.

Table 20. Management Access Options

Option	Description
Telnet access	By default, this option is disabled (inactive).
Telnet port	This field lists the default Telnet port of 23. You can manually change this port number, if required.
SSH access	By default, this option is enabled (active).
SSH port	This field lists the default SSH port of 22. You can manually change this port number if required.
HTTP access	This option is enabled by default.
HTTP port	This field lists the default HTTP port of 80. You can manually change this port number if required.
HTTPS access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the device.
HTTPS port	This field lists the default HTTPS port of 443. You can manually change this port number if required.
Certification Verification	This notes whether the security certificate linked to the HTTPS settings has been passed or not.
Auto Provisioning?	Enabled by default. Auto Provisioning allows configuration of multiple ZoneFlex 7025s at once.

3. If you want the Multimedia Wi-Fi Wall Switch to be accessible for management from outside of the local network, select the **Allow Remote Management** check box.
4. If you want to allow specific IP addresses only to be able to access the device for remote management, select the **Limited by IP Range** check box, and then specify the IP addresses or IP address ranges that are allowed to access the device by entering the IP address and network mask combination. You can specify up to four sets of IP address ranges.
5. Click **Update Settings**.

You have completed configuring the options for management access.

## Enabling Logging and Sending Event Logs to a Syslog Server

If you have a syslog server on the network, you can configure the Multimedia Wi-Fi Wall Switch to send the device logs to the server. You will need to enable logging, and then configure the ZF7025 to send logs to the syslog server.

1. Go to **Administration > Log**. The Administration :: Log page appears.
2. Look for **Log Status**, and then click **Enabled**.
3. After enabling logging, configure the following options:
  - **Syslog Server Address [Optional]**: To enable the Multimedia Wi-Fi Wall Switch to send messages to a syslog server as they appear, enter the IP address of the syslog server.
  - **Syslog Server Port**: By default, the syslog port number is 514. If the syslog server is using a different port, enter that port number in this field.
4. Click **Update Settings** to save and apply your changes.

Figure 32. The Administration > Log page

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

LOGOUT

**Administration :: Log**

Need Help?

Log Status: ☒ Enabled ☐ Disabled

Syslog Server Address: 0 . 0 . 0 . 0

Syslog Server Port: 514

**Current Log** Refresh

Jul 24 03:40:23	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:26	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:28	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:31	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:34	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:47	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:50	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:53	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:56	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:40:59	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:02	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:05	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:08	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:11	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:15	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:27	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:30	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:33	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...
Jul 24 03:41:36	RuckusAP	local0.debug	udhcpc[438]:	Sending discover...

**Ruckus** WIRELESS Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

## Sending a Copy of the Log File to Ruckus Wireless Support

The Support Info log consists of the configuration and run-time status of the Multimedia Wi-Fi Wall Switch and can be useful for troubleshooting. You have three options for sending a copy of the current log file to Ruckus Wireless Support:

- Save a copy to your local PC, then attach it to an email message and send it to Ruckus Wireless Support
- Set up a connection to an FTP site
- Set up a connection to a TFTP site

### To take advantage of these options

1. Go to **Maintenance > Support Info**. The Maintenance :: Support Info page appears.
2. Review the Upload Method options.
3. To upload a copy of the support info file to an FTP or TFTP server, click TFTP or FTP option. Clicking the FTP option prompts you to enter a User ID and Password.
4. In **Server Address**, enter the FTP or TFTP server IP address.
5. In **Filename**, enter a name for this file that you are saving.



---

**NOTE:** Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host".

---

6. Click **Upload Now**.

## Saving a Copy of the Current Log to Your Computer

You can also save a copy of the current log to your own computer, if needed.

1. Go to **Maintenance > Support Info**. The Maintenance :: Support Info workspace appears.
2. Review the *Transfer Method* options.
3. Click the **Save to local computer** option. The following text appears below the Transfer Method options:  
`Download: supportinfo.txt`
4. Right-click the `supportinfo.txt` link.
5. When the Save As dialog box appears, change the destination directory and change the file name if you prefer.
6. Click **Save** to save the file to your computer.

## Upgrading the Firmware

You can use the Web interface to check for software updates/upgrades for the firmware built into the Multimedia Wi-Fi Wall Switch. You can then apply these updates to the device in one of two ways:

- Manually updating on an as-needed basis, or;
- Automating the update by setting an update schedule.

Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now.

By default, the automatic upgrade option is active, and will check the Ruckus Wireless update server every 12 hours.

To get started with upgrading the firmware, go to **Maintenance > Upgrade**. When the **Maintenance > Upgrade** options appear, decide which upgrade method to use. Each of the upgrade options listed on the Upgrade page are discussed in the succeeding sections.

Figure 33. The Maintenance > Upgrade page

Ruckus 7025 Multimedia Wall Pluggable Wireless AP

LOGOUT

**Maintenance :: Upgrade**

Need Help?

Upgrade Method: ☐ TFTP ☒ FTP ☐ Web ☐ Local

**FTP Options**

Firmware Server: fwupdate1.ruckuswireless.com

Port: 21

Image Control File: zf7025\_910\_cntrl.rcks

Username: zf7025

Password: ●●●●●●●●

Auto Upgrade? ☐ Enabled ☒ Disabled

Changes made to this area apply to the Automatic Firmware Update settings as well.

**WARNING:** Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your device until the upgrade finishes.

Perform Upgrade Save parameters only Restore previous settings

Ruckus WIRELESS Ruckus 7025 Multimedia Wall Pluggable Wireless AP

© Copyright 2009 Ruckus Wireless

## Upgrading Manually via FTP or TFTP

1. In the **Upgrade Method** options, click **FTP** or **TFTP**.

2. Click the host name field, and then type the URL of the server. Or click the IP address field, and then type the IP address of the server.



---

**CAUTION:** Do not change any of the Image Control File, Username, or Password entries.

---

3. Click **Perform Upgrade**. A status bar appears during the upgrade process.
4. After the upgrade is completed, you must manually reboot the Multimedia Wi-Fi Wall Switch.

## Upgrading Manually via the Web

1. In the **Upgrade Method** options, click **Web**.
2. Click the **Web Options URL** field, and then type the URL of the download Web site. Remember to start the URL with the **http://** prefix.
3. You can change the Image Control File filename extension as noted here:
  - Replace any file names ending in **.rcks** with the **.html** extension
  - Replace any file names ending in **.f17** with the **.html** extension



---

**CAUTION:** Do not change the **Username** or **Password** entries.

---

4. Click **Perform Upgrade**. A status bar appears during the upgrade process.
5. After the upgrade is completed, you must manually reboot the Multimedia Wi-Fi Wall Switch.

## Upgrading Manually via Local File

If you have already saved a firmware file on your local computer, you can upgrade directly using the Web interface.

1. In the **Upgrade Method** options, choose **Local**.
2. Click the **Browse** button and locate the file on your local computer.
3. Select the file and click **OK**.
4. Click **Perform Upgrade**. A status bar appears during the upgrade process.
5. After the upgrade is completed, you must manually reboot the AP.

## Scheduling Automatic Upgrades

Configure the automatic upgrade schedule to enable the Multimedia Wi-Fi Wall Switch to check a firmware upgrade source for available downloads and upgrade its firmware automatically.

Figure 34. The Auto Upgrade section on the Upgrade page

The screenshot shows the 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' configuration page. The left sidebar contains navigation links: Status (Device, Internet, Wireless), Configuration (Device, Internet, Wireless, LAN Ports), Maintenance (Upgrade, Reboot / Reset, Support Info), and Administration (Management, Diagnostics, Log). The main content area is titled 'FTP Options' and includes fields for 'Firmware Server' (fwupdate1.ruckuswireless.com), 'Port' (21), 'Image Control File' (zf7025\_910\_cntrl.rcks), 'Username' (zf7025), and 'Password' (masked). Below these is the 'Auto Upgrade?' section, which is highlighted with a red box. It contains radio buttons for 'Enabled' (selected) and 'Disabled'. Below the radio buttons are two dropdown menus: 'Interval to Check for Software Upgrade' (set to 12 Hours) and 'Schedule Reboot Time after Upgrade' (set to Any Time). A red-bordered box contains a warning message: 'Changes made to this area apply to the Automatic Firmware Update settings as well. WARNING: Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your device until the upgrade finishes.' At the bottom of the red box are three buttons: 'Perform Upgrade', 'Save parameters only', and 'Restore previous settings'. The footer of the page shows the Ruckus logo and the text 'Ruckus 7025 Multimedia Wall Pluggable Wireless AP' and '© Copyright 2009 Ruckus Wireless'.

#### To configure automatic upgrades

1. In the **Upgrade Method** options, click the button for your preferred upgrade method.



**NOTE:** Automatic Upgrade is only available if you select TFTP, FTP, or Web as the **Upgrade Method**.

2. In **Firmware Server** or **URL** (depending in whether selected TFTP/FTP or Web as the upgrade method), type the host name, IP address, or URL where the Multimedia Wi-Fi Wall Switch can automatically download the firmware.



**CAUTION:** Do not change any of the Image Control File, Username, or Password entries.

3. In **Auto Upgrade**, verify that the **Enabled** option is selected (active).
4. In **Interval to Check for Software Upgrade**, select the time interval when you want the Multimedia Wi-Fi Wall Switch to automatically check for firmware upgrades. Options range from 1 hour to 4 weeks.

5. In **Schedule Reboot Time after Upgrade**, select the time (GMT) when the Multimedia Wi-Fi Wall Switch will be rebooted automatically after the new firmware is downloaded. The Multimedia Wi-Fi Wall Switch requires a reboot to complete the upgrade process. Ruckus Wireless recommends that you select an offpeak hour so fewer users would be affected by the reboot.
6. Specify when you want the Multimedia Wi-Fi Wall Switch to check for firmware upgrades:
  - To check immediately, click **Perform Upgrade**. If a firmware upgrade is available, the Multimedia Wi-Fi Wall Switch will download it from the specified source immediately. A status bar appears, which displays the progress of the upgrade process. To complete the upgrade process, it will reboot automatically at the reboot time that you specified.
  - To check for available firmware upgrades at the time interval that you specified, click **Save parameters only**. The Multimedia Wi-Fi Wall Switch's clock starts counting down to the specified time interval and, when the time interval is reached, checks the firmware upgrade source and downloads any available firmware upgrade. To complete the upgrade process, it will reboot automatically at the reboot time that you specified.

You have completed the automatic upgrade configuration.



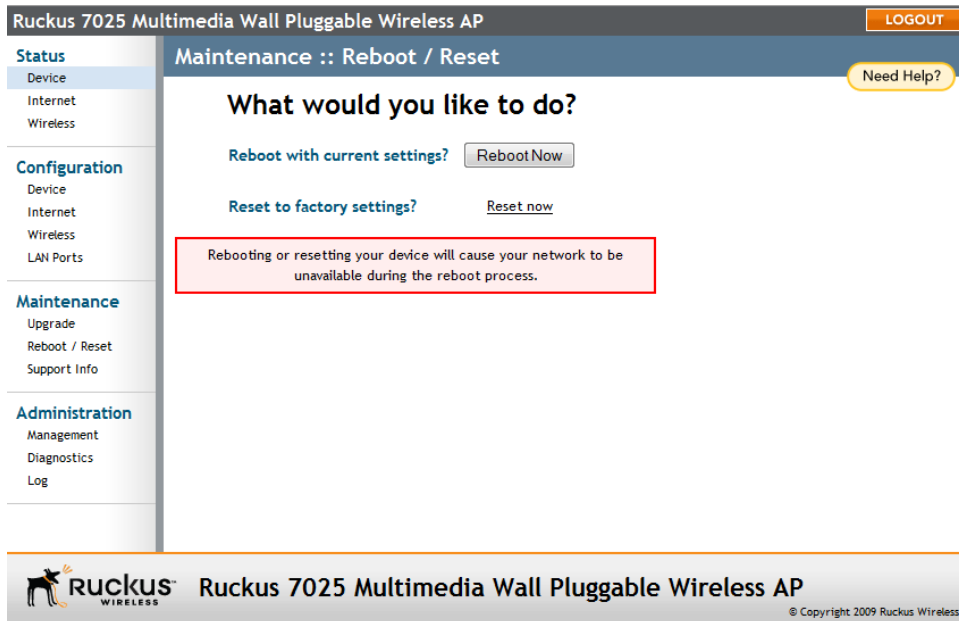
## Rebooting the Multimedia Wi-Fi Wall Switch

You can use the Web User interface to prompt the Multimedia Wi-Fi Wall Switch to reboot, which simply restarts the Multimedia Wi-Fi Wall Switch without changing any of the current settings.



**CAUTION:** Rebooting the Multimedia Wi-Fi Wall Switch will disrupt network communications on any currently active WLANs.

Figure 35. The Maintenance > Reboot/Reset page



### To reboot the Multimedia Wi-Fi Wall Switch

1. Go to **Maintenance > Reboot/Reset**. The Maintenance :: Reboot/Reset page appears.
2. Click **Reboot Now**. After a brief pause, you will be automatically logged out of the Multimedia Wi-Fi Wall Switch.

After a minute or so, you should be able to log back into the Multimedia Wi-Fi Wall Switch, which verifies that the reboot was successful. You can also check the LEDs on the Multimedia Wi-Fi Wall Switch to verify the status of the device.

## Resetting to Factory Defaults



**WARNING:** DO NOT reset the Multimedia Wi-Fi Wall Switch to factory defaults, unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately reconnect the restored Multimedia Wi-Fi Wall Switch to your computer, to reconfigure it for Wi-Fi network use.

You can use the Web User interface to restore an inoperative Multimedia Wi-Fi Wall Switch to its factory default settings, which will completely erase the configuration currently active in the device. Note, too, that this will disrupt all wireless network communications through this device.

### To reset the Multimedia Wi-Fi Wall Switch to factory defaults

1. Go to **Maintenance > Reboot/Reset**. The Maintenance :: Reboot/Reset page appears.
2. Click **Reset Now** (next to *Restore to factory settings?*).



**NOTE:** You can also use the Hard Reset button on the left side of the AP to restore it to factory defaults. Refer to [“Reset Buttons”](#) on [page 9](#) for more information.

After a brief pause, you will be automatically logged out of the Multimedia Wi-Fi Wall Switch. You must now disconnect the Multimedia Wi-Fi Wall Switch reconnect it to your computer, as described in [“Step 1: Prepare the Administrative Computer”](#) on [page 12](#). At this time, you can restore the network settings, then replace it in your site for full network use.

## Running Diagnostics

Two network connection diagnostic tools – PING and traceroute – have been built into the Multimedia Wi-Fi Wall Switch to help you check network connections from the Web interface.

### To run diagnostics for network troubleshooting

1. Go to **Administrator > Diagnostics**. The Administrator :: Diagnostics page appears. Two options are available:
  - Ping
  - Traceroute
2. Click the text field by the option you want to activate, and type the network address of a site you wish to connect to.
3. Click **Run Test**.

The results appear in the text field below each option.

Figure 36. Pinging ruckuswireless.com

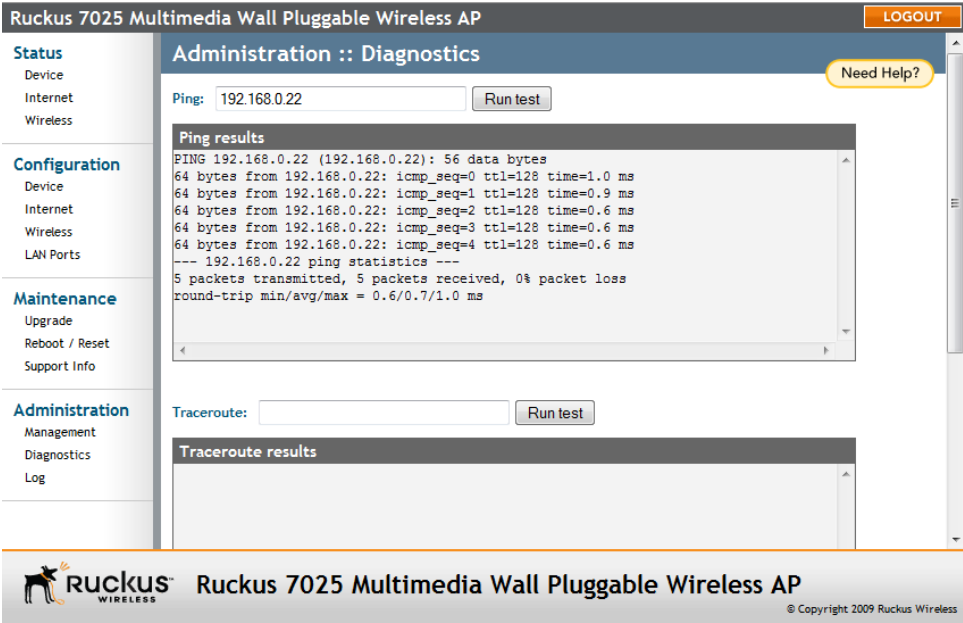
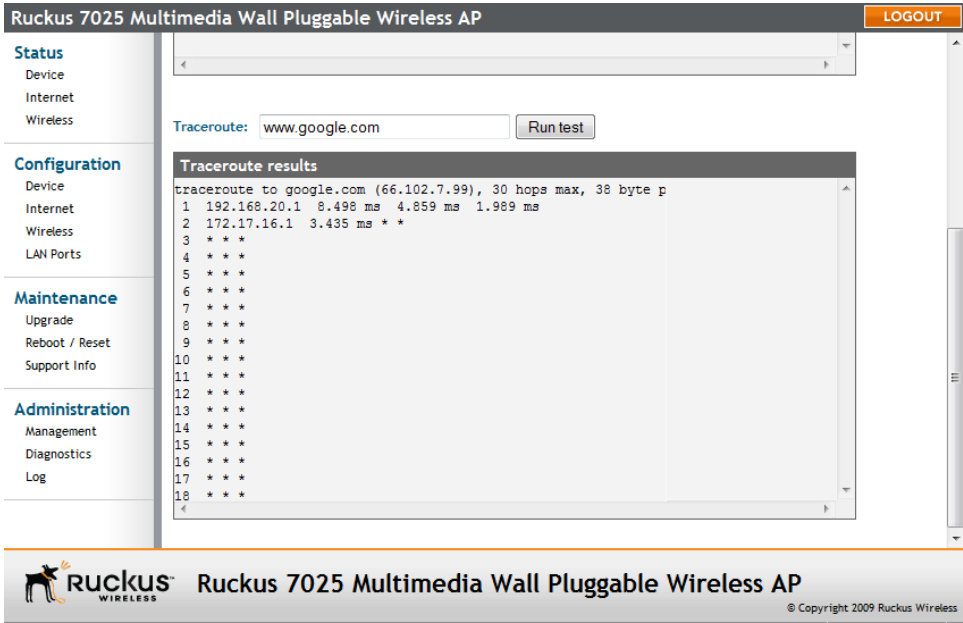


Figure 37. Running traceroute on ruckuswireless.com



## Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at <http://support.ruckuswireless.com/>. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.

# Index

## Numerics

802.1X, 42  
802.1X settings, 42

## A

access control, 46–47  
administrative login, 53  
advanced wireless settings, 32  
AeroScout, 32, 53

## B

broadcast SSID, 36

## C

changing the login settings, 26  
country code, 32, 53

## D

default IP address, 27  
default user name and password, 22  
device location, 26  
device name, 26  
device settings, 26  
DHCP, 27, 29  
    release, 29  
    renew, 29  
diagnostics, 64  
Dynamic VLAN, 37

## E

encryption, 37  
event logs, 57

## F

factory defaults  
    resetting, 9, 64  
firmware upgrade, 59

## H

Help, 24

## I

installation, 11  
Internet settings, 27  
IP address, 27

## L

LAN ports, 4, 48  
    configuration, 48  
LAN4, 6  
LAN5/Uplink, 5, 7, 48  
LEDs, 8  
Log Out button, 23–24  
logging in, 22  
login settings, 53  
logs, 58

## M

management access, 55  
menu, 23

## N

NTP server, 28

## P

package contents, 3  
pass through port, 4–5, 7  
passphrase, 39

- PING, 64
- PoE injector, 13
- port-based VLAN, 48, 50
- protection mode, 35
- punch down block, 5, 7, 19

## R

- rebooting, 9, 63
- releasing DHCP, 29
- renewing DHCP, 29
- reset buttons, 9

## S

- SSID, 37
- static IP, 29
- static IP address, 27
- syslog, 57
- syslog server, 57

## T

- tabs, 23
- temperature update, 26
- threshold, 37
- traceroute, 64
- transmit power, 35

## U

- upgrading firmware, 59
- user name, 26

## V

- VLAN, 48–49
  - dynamic, 37

## W

- Web interface, 22
- WEP, 38
- wireless availability, 36
- wireless channel, 53
- wireless mode, 32, 53

- wireless security
  - 802.11X, 42
  - WEP, 38
  - WPA, 40
- wireless settings, 31
- workspace, 23
- WPA, 40
- WPA-Auto, 41

## Z

- ZF7025
  - EU model, 6
  - US model, 3
- ZF7025-EU
  - front panel, 6
  - rear panel, 7
- ZF7025-US
  - front panel, 3
  - rear panel, 4